NASA HQ
Office of Protective Services
Counterintelligence Division

"Detect, Deter, and Neutralize"

NASA Counterintelligence Executive Brief

May 7, 2013

Subject: Foreign Intelligence Services Take Advantage of Ethnic Ties to Recruit Spies

Counterintelligence Executive Brief

This Counterintelligence Executive Brief (CIEB) was prepared by Counterintelligence Special Agent Arthur R. Payton, NASA HQ. The intent of this CIEB is to provide information to NASA personnel to ensure clear understanding of indicators of counterintelligence concern. The NASA HQ Counterintelligence Office is located in Suite CV75 can be contacted at (202) 358-4645.

EXECUTIVE SUMMARY

NASA employees, via international partnerships, conferences/symposia, and other venues have a great number of contacts with people from other countries. These partnerships greatly benefit our people, agency and nation; however, these contacts can also be exploited by foreign intelligence services. Foreign intelligence officers frequently attend open conferences, trade show, symposia, etc., to spot potential "targets" (people with access to information the intelligence officer's country is attepting to acquire). One way foreign intelligence services exploit such relationships is by spotting and targeting US Government employees who immigrated to the United States from "the old country" and appeal to their shared bonds (language, culture, history, religion, etc.) in an attempt to establish personal or professional relationships. These relationships can progress to the point where the new "friend" asks for information an employee has access to (usually unclassified/non-sensitive information…at first). Once "hooked" into providing information, however innocuous, this can lead to requests for more sensitive and even classified information. One of the best ways to prevent oneself from falling into such a trap is by reporting to your servicing NASA Counterintelligence Office (located at the HQ and each Center) any suspicious requests for information.

BACKGROUND

In the world of intelligence and espionage, there's virtually no such thing as a "friendly country." Countries collect information from friends and foes alike that will help them militarily, diplomatically and economically. Even countries that are long-time allies of ours are, from time to time, caught committing espionage against the United States; often by recruiting government employees with information they seek or by accepting "volunteers" offering to provide the information. Social cultivation of government employees by foreign intelligence services is a tried and true method that allows intelligence officers to spot and assess potential targets for recruitment. Often a foreign intelligence service will seek out people who have ties to their country and appeal to their sympathies for that country. The best example of this is targeting people who were born in, raised in and who speak the language of the "motherland/fatherland" but who become citizens of the targeted country…immigrants. An appeal is frequently made to the "recruit" that their nation of origin needs their help to catch up to/gain parity with the adopted country. People who have been recruited this way have caused great damage to the United States by providing their foreign intelligence service handlers classified and sensitive US Government and "trade secret" information. Not only is the damage caused by these great in terms of loss to the United States and the taxpayer, the personal consequences are also severe to include loss of security clearance, loss of job and/or incarceration.

A May 2013 article that appeared in an Australian newspaper (attached) detailed the story of an Australian government employee who lost his security clearance and job after he was found to have had repeated unreported contact with foreign intelligence officers. The Australian government employee had immigrated to Australia from South Korea and was targeted by a known South Korean intelligence officer who was posted in Australia. A very close social

relationship was developed between the two and, eventually, the employee passed on to the South Korean intelligence officer trade negation information to which he had access based on his duties as an Australian government employee. This relationship was uncovered by Australian intelligence authorities who warned the employee that his South Korean embassy friend was an intelligence officer. Even after the warning the employee continued his association with the South Korean intelligence office to include engaging in clandestine meetings. Although no outright espionage was proved, the security suitability concerns raised by the employee's actions led to his losing his government security clearance and being fired from his job.

NASA COUNTERINTELLIGENCE PERSPECTIVE

Though the referenced example involved an Australian government employee, this is just a recent example of a government employee being targeted by a foreign intelligence service based on the employee's country of birth. Due to our international partnerships, participation in overseas conferences/symposia, etc., NASA employees who are naturalized citizens are at added risk for social cultivation attempts by the intelligence services of their nation of origin. One must be on guard when establishing personal or professional relationships with foreign nationals and report suspicious contacts to NASA Counterintelligence officials.

Reportable Foreign Intelligence Contacts, Activities, Indicators, and Behaviors
(Borrowed from Department of Defense Directive 5240.6, CI Awareness and Reporting)

1. When not related to official duties, contact with anyone known or believed to have information of planned, attempted, actual, or suspected espionage, sabotage, subversion, or other intelligence activities against NASA facilities, organizations, personnel, or information systems.

2. Contact with an individual who is known or suspected of being associated with a foreign intelligence or security organization.

3. Visits to foreign diplomatic facilities that are unexplained or inconsistent with an individual's official duties.

4. Acquiring, or permitting others to acquire, unauthorized access to classified or sensitive information systems.

5. Attempts to obtain classified or sensitive information by an individual not authorized to receive such information.

6. Persons attempting to obtain access to sensitive information inconsistent with their duty requirements.

7. Attempting to expand access to classified information by volunteering for assignments or duties beyond the normal scope of responsibilities.

8. Discovery of suspected listening or surveillance devices in classified or secure areas.

9. Unauthorized possession or operation of cameras, recording devices, computers, and communication devices where classified information is handled or stored.

10. Discussions of classified information over a non-secure communication device.

11. Reading or discussing classified or sensitive information in a location where such activity is not permitted.

12. Transmitting or transporting classified information by unsecured or unauthorized means.

13. Removing or sending classified or sensitive material out of secured areas without proper authorization.

14. Unauthorized storage of classified material, regardless of medium or location, to include unauthorized storage of classified material at home.

15. Unauthorized copying, printing, faxing, e-mailing, or transmitting classified material.

16. Improperly removing classification markings from documents or improperly changing classification markings on documents.

17. Unwarranted work outside of normal duty hours.

18. Attempts to entice co-workers into criminal situations that could lead to blackmail or extortion.

19. Attempts to entice NASA personnel or contractors into situations that could place them in a compromising position.

20. Attempts to place NASA personnel or contractors under obligation through special treatment, favors, gifts, or money.

21. Requests for witness signatures certifying the destruction of classified information when the witness did not observe the destruction.

22. Requests for NASA information that make an individual suspicious, to include suspicious or questionable requests over the internet.

23. Trips to foreign countries that are:

a. Short trips inconsistent with logical vacation travel or not part of official duties.

b. Trips inconsistent with an individual's financial ability and official duties.

24. Unexplained or undue affluence.

a. Expensive purchases an individual's income does not logically support.

b. Attempts to explain wealth by reference to an inheritance, luck in gambling, or a successful business venture.

c. Sudden reversal of a bad financial situation or repayment of large debts.

WAtoday.com.au

Friends, spies and espionage

Published: May 2, 2013 - 1:00AM

Yeon Kim was crazy about soccer. Born, raised and in part educated in Asia's most successful World Cup soccer nation, South Korea, he always loved the game. And for more than a decade this respected Australian government agricultural trade analyst spent his Saturday afternoons playing social soccer at Kambah Oval in Canberra's southern suburbs.

The Saturday matches were informal but competitive. The players, a mix of Australian locals and some foreigners from Canberra's diplomatic community, generally divided into two evenly matched teams, would usually play for a couple of hours.

Occasionally there were disputes on the field, and Kim complained about "South American players … who had hot tempers and were spoiling his enjoyment". Generally, however, the mood was relaxed and friendly and Kim regarded Saturday soccer as one of his favorite pastimes. But in late 2010 and through 2011 not everyone at Kambah Oval was focused on the world game.

Surveillance officers from the Australian Security Intelligence Organization were sitting on the sidelines or eating sandwiches and drinking coffee in the car park while they discreetly watched and photographed Kim and another soccer enthusiast, South Korean embassy minister-counselor Hoo-Young Park.

Park is a senior officer of South Korea's National Intelligence Service; in ordinary parlance, a spy. Kambah Oval was a somewhat incongruous focus in a major ASIO counter-espionage investigation.

An economist and trade policy wonk, Kim migrated to Australia in 1982, aged 20 and has lived in Canberra since 1994. He speaks fluent Korean and has long mixed with Canberra's small Korean community, including officers of the South Korean embassy.

A Sydney University economics graduate, Kim completed a doctorate at the Australian National University in 2000. His PhD thesis dealt with the impact of agricultural trade liberalization on the Korean economy.

He served as an economic policy analyst with the Treasury from 2000 to 2004 before moving to the Australian Bureau of Agricultural and Resource Economics and Sciences (ABARES), which is part of the Department of Agriculture, Fisheries and Forestry.

Kim's work with ABARES covered analytical research and economic modeling of multilateral and bilateral agricultural trade policy issues, World Trade Organization and free trade agreement-related agricultural market access issues. He was the principal author of a 2009 ABARES study of the Korean beef market.

His publicly available CV also shows he was involved in ''international capacity building and training activities for foreign governments' officials''.

Kim was introduced to Park by another South Korean diplomat at Canberra Airport when the ABARES economist was returning home from an overseas trip in June 2009. They met again at a Korean community gathering - probably at a Korea Day celebration in Canberra's Glebe Park- on October 3, 2009. Park apparently mentioned that he enjoyed soccer and Kim told him about his Saturday soccer games and invited Park to join in.

Soon after, Park and his son began to play soccer with the group at the Kambah Oval and, in time, brought a few other Koreans, apparently embassy officers, to play.

Kim and Park and their families began to socialize regularly, often with two other Korean migrants, one a Canberra businessman and another who had served as national coach for the Korean women's World Cup soccer team. The four families used to meet up at the Saturday soccer games and talk about ''sport, politics, economic issues, national events, and children's education''.

While Kim and Park played soccer, and talked over an occasional lunch and at South Korean embassy functions, ASIO was watching and probably listening.

The South Korean diplomat was well known to ASIO. Posted to Canberra under diplomatic cover, he was declared by the South Korean government as an NIS liaison officer, continuing a co-operative relationship of more than 30 years between the Australian and South Korean intelligence communities.

It is understood that Park visited Australia's intelligence agencies, especially the Office of National Assessments and ASIO. Under the gentleman's agreements governing such relationships, Park and other NIS officers at the South Korean embassy were not to engage in covert intelligence collection in Australia.

ASIO was concerned, however, that the NIS was breaking the rules and trying to ''cultivate Australian officials and public servants to obtain sensitive information'' that would give an advantage to South Korea in free trade agreement negotiations between Canberra and Seoul.

While Kim was not a trade negotiator, his expertise brought him close to the free trade agreement talks as Australia hoped to secure greater access to Korea's potentially lucrative beef market. Indeed, Kim participated in one session of the third round of trade talks held in Canberra in December 2009.

However, Kim's public service career began to unravel when in mid-2010 ASIO received information that he had been meeting a South Korean diplomat known to be an NIS officer. Kim had not declared his contacts with the diplomat - understood to be Park - in accordance with government security policy.

After initial inquiries, ASIO asked the Agriculture Department to have Kim complete a security questionnaire on August 5, 2010. He was required to complete the questionnaire immediately, with a break for lunch. He answered questions about his awareness of government security procedures and his contact with foreign government officials.

He later recalled he felt "anxious and panicky and he had no opportunity to reflect on the questions or to check his diary".

Two months later, on October 7, Kim was summoned without warning to an interview with two ASIO officers. When he entered the interview room he was "worried, scared and confused, asking himself 'why me?' and noting the high quality recording machine in place in the room".

Kim said he found it difficult to concentrate on the ASIO officers' questions and said that if the questions had been clearer, some of his answers would have been different.

Asked whether he had discussed the free trade agreement negotiations with Park, he answered "No." Much later he acknowledged that he had discussed the negotiations in lengthy conversations in December 2009, but insisted he had referred only to publicly available information and nothing that could be regarded as sensitive.

Towards the end of the interview ASIO told Kim that Park and three other South Korean diplomats he had had contact with were NIS officers. He was warned that intelligence officers could be "very subtle and very clever in the way they operate" and to report any future dealings or contact with foreign diplomats. Kim later said that when ASIO told him Park was an NIS officer, "he realized something was wrong and his relationship with Mr Park was a serious problem".

Despite this, Kim continued to meet Park, indeed at least as late as May 2011, but did not report these contacts to ABARES or ASIO. He later explained this failure because of "the very casual nature of their contact at soccer, which was insignificant and bore no relationship to [his] work" and because "he had a heavy workload and procrastinated".

Kim heard nothing more from ASIO for 11 months. Then, on September 15, 2011, ASIO Director-General David Irvine issued an adverse security assessment of Kim "after finding that he had had contact with successive NIS officers who he had not reported, as required by Australian government policy".

ASIO alleged that Kim was involved in clandestine contact with, and provided "sensitive" and "privileged" information to Park and that his conduct amounted to participation in acts of "foreign interference".

ASIO alleged that Kim had been "deceptive" in his responses to questioning, and that there was a "specific threat" to information held by ABARES including information from other government agencies.

ASIO recommended that his secret level security clearance be revoked, effectively ending his career as a public servant.

Faced with losing his job with ABARES, and indeed being effectively banned from work with the Australian Public Service, Kim sought a review of ASIO's assessment by the Administrative Appeals Tribunal.

At a hearing of the tribunal's Security Appeals Division in mid-2012, ASIO's lead investigator, a veteran of 24 years with the security agency, observed that Australian public servants were

"regularly targeted" by foreign intelligence services because they were potentially valuable sources of information.

"Intelligence officers participate in social and other groups, befriend a person and then seek to cultivate that relationship. ASIO's assessment is that [Kim] has been successfully cultivated by the NIS."

Many details of ASIO's investigation remain classified, but it is more likely than not that they extended to access of telecommunications data and telephone interception, as well as physical surveillance.

On the basis of its investigations and observations, ASIO argued that Kim's "actions and associations demonstrate he is not sufficiently honest and trustworthy to have access to classified, caveated government information or to hold a SECRET level security clearance".

Kim denied any improper dealings with South Korean diplomats, saying that his relations with them were purely social in nature, and that any discussion of trade issues was confined to non-sensitive or publicly available information.

However, last August the Administrative Appeals Tribunal upheld ASIO's adverse security assessment. The tribunal observed that Kim was "highly intelligent" and found it "hard to accept that a person of his intelligence, and with knowledge of security requirements that he professed to have, would not have found Mr Park's obvious interest in [Kim's] involvement in the third round of FTA negotiations suspicious."

The tribunal said that it had been "provided with [classified] evidence … indicating that [Kim] arranged to meet with Mr Park in a clandestine manner in order to avoid scrutiny. Such actions inevitably raise doubts about [Kim's] loyalty to Australia."

Reflecting on Kim's own testimony at its hearing, the tribunal observed that Kim may have had "a misguided view of himself in … a bridging role" between the Australian and South Korean governments and that there were "doubts … about his having divided loyalties between the country of his birth and the county of his adoption".

The tribunal expressed itself "satisfied that [Kim's] actions … were detrimental to the interests of Australia".

In affirming ASIO's assessment, the tribunal expressed sadness "knowing the likely effect on [Kim's] career" but concluded that the responsibility was his. Kim has appealed the tribunal's decision to the Federal Court.

Intelligence and security professionals will find little that is remarkable in this story. In many respects it looks like a textbook case of recruitment by a foreign intelligence service of a source of potentially valuable information. At best Kim's actions appear remarkably naive.

Factors such as common language, cultural background and social interaction are often exploited by intelligence officers. China's very active foreign intelligence services are well known for focusing their efforts on members of the Chinese diaspora, and many other intelligence services pursue similar strategies.

Nor would South Korea be the first or the last ''friendly'' nation to engage in covert intelligence activity in Australia - Israel, France, Japan, Taiwan and indeed the United States have all done this in the past.

What is surprising, however, is that ASIO appears to have put helping a foreign intelligence service to avoid embarrassment ahead of Australia's trade and economic interests.

By any standards it is remarkable that ASIO, with the approval of former attorney-general Nicola Roxon, should have gone into the Federal Court to argue for the suppression of the identities of foreign intelligence officers who have been actively working against Australia's trade interests so that they can continue their clandestine careers in the future.

No doubt a case can be made that continuing co-operation between the Australian intelligence community and South Korea's National Intelligence Service serves Australian national security interests.

However, as Kim's lawyers argued to the Federal Court, ''a reasonable observer might well take the view that it is a matter of legitimate interest to citizens of Australia to know if agents of friendly nations have engaged in activities inconsistent with diplomatic cover involving an attempt to cultivate a senior public servant in Australia''.

Fortunately, ASIO's desire to protect its Korean intelligence partner, even when that partner has crossed the boundaries of acceptable conduct, has not been accepted by Federal Court judge Lindsay Foster and much of the story can now be published.

As for Dr Kim, whatever the precise details of his case and the eventual outcome of his Federal Court appeal, he no doubt wishes he had stuck strictly to the pleasures of weekend soccer.

This story was found at: ***http://www.watoday.com.au/national/friends-spies-and-espionage-20130501-2iszb.html***